UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,175	07/29/2003	Alan D. Boulanger	RPS920030010US1	7176

25299 7590 03/12/2007

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
AVELLINO, JOSEPH E	
ART UNIT	**PAPER NUMBER**
2143	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/629,175	BOULANGER ET AL.	
	Examiner	Art Unit	
	Joseph E. Avellino	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/29/2003, 10/18/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are presented for examination; claims 1, 11, 20, 25, and 30 independent.

Information Disclosure Statement

2. The IDS's submitted July 29, 2003 and October 18, 2004 have been considered. See enclosed PTO-1449.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 11-24 are rejected under 35 U.S.C. 101 because they are not tangible embodiments of the invention.

4. Referring to exemplary claim 11, the claim recites a system which has a table and a controller which adjusts values in the table, both of which can be implemented in merely software. As such the system is just software, per se, and is not tangibly embodied on any device or tangible medium. Correction is required to provide the intrusion detection system is tangible (i.e. device).

5. Referring to exemplary claim 20, the claim is directed to a program product which includes a medium. MPEP 2106 that computer-related inventions are implemented on a tangible, computer-readable medium. As originally claimed, the medium can be construed as an intangible medium (i.e. carrier wave), or a non-computer-readable medium (i.e. a piece of paper). As such, correction is required to ensure that the program product is tangibly embodied on a computer-readable medium.

6. Any claim not expressly discussed above is rejected for similar reasons as stated above.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 5, 6, 8, 11, 12, 14-18, 20-31, 34, and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Shanklin et al. (USPN 6,487,666) (cited by Applicant in IDS) (hereinafter Shanklin).

8. Referring to claim 1, Shanklin discloses a method for detecting unauthorized reconnaissance or scanning (i.e. detect attacks on a local network) of a computer network comprising the acts of:

monitoring communications within the network (col. 1, lines 27-32);

detecting predefined sequence of packets flowing within communications (i.e. count number of SYN packets without SYN-ACK packets in a given time period) (col. 6, lines 15-20); and

issuing an alert indicating unauthorized scanning if the predefined packet sequence is detected (i.e. an alarm is generated) (col. 6, lines 15-20).

9. Referring to claim 2, Shanklin discloses the monitoring is done with a selected network device (i.e. intrusion detection system sensor 11) (col. 2, lines 35-45).

10. Referring to claim 5, Shanklin discloses the sequence of packets are TCP/IP packets (col. 5, lines 50-55).

11. Referring to claim 6, Shanklin discloses the use of TCP/IP and therefore inherently discloses the use of TCP SYN/ACK, and TCP RST packets (See RFC 793: Transmission Control Protocol, section 3.1 which deals with header formats; and section 3.4 which deals with the establishment of a connection).

12. Referring to claim 8, Shanklin discloses sending a message to an administrator (i.e. report the attack) (col. 1, lines 35-38).

13. Claims 11, 12, 14-18, 20-31, 34, and 35 are rejected for similar reasons as stated above.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 7, 9, 10, 13, 19, 32, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin.

16. Referring to claim 7, Shanklin discloses the invention substantively as described in claim 6. Shanklin does not specifically disclose that a single device generates the TCP SYN packet, the TCP RST packet and received the TCP SYN/ACK packet, however this is a common set up of TCP/IP 3-way handshaking, and is well known and can be found in RFC 793. By this rationale, "Offical Notice" is taken that both the concepts and advantages of providing for a device generating the SYN and RST packets and received the SYN-ACK packet is well known and expected in the art. It would have been obvious to one of ordinary skill in the art to modify the teaching of Shanklin to have one device generate a SYN and RST packet and receive the SYN-ACK packet, since this is how a connection would be established (via the SYN and SYN-ACK packet) and terminated or reset (via the RST packet) as seen in RFC 793 (section 3.4).

17. Referring to claims 9 and 10, Shanklin does not specifically disclose blocking future packets from network computers having predefined characteristics, or rate-limiting flows of packets, however these are common preventative measures to ensure an attack on a network is not successful. By this rationale, "Official Notice" is taken that both the concepts and advantages of providing for blocking or rate limiting packets is well known and expected in the art. It would have been obvious to one of ordinary skill in the art to modify the teaching of Shanklin to include blocking or rate-limiting packets, since Shanklin discloses the use of firing an alarm, however does not specifically

discuss what the alarm does. This would lead one of ordinary skill in the art to search the art to find methods of network defense, eventually finding the well known features of rate-limiting and blocking packets from specific addresses.

18. Referring to claim 13, Shanklin discloses the invention substantively as described in claim 11. Shanklin does not disclose the actual values of the state codes of the table in which the packets are observed, however Shanklin does disclose monitoring a particular sequence of packets (col. 5, lines 13-33). Therefore there inherently must be a mechanism within Shanklin which is capable of determining if the particular sequence of packets fits this particular "signature" (i.e. a sequence of packet type A, followed by 0 or more packets of any type, followed by two packets of type B, followed by 0 or more packets of any type, followed by a packet of type C, will match the expression A.*BB.*C as given in an example in col. 5, line 29. Therefore the computer must be able to determine when a first of the sequence, a second of the sequence, and the last of the sequence of predefined packets has been received. The state codes chosen do not provide any patentable distinction and are mere design choice.

19. Claims 19, 32, and 33 are rejected for similar reasons as stated above.

Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin in view of Etheridge et al (US 20040054925) (hereinafter Etheridge).

20. Referring to claim 3, Shanklin discloses the invention substantively as described in claim 1. Shanklin further discloses counting a particular type of packet in a certain time period in order to determine whether to fire an alarm (i.e. if SYN packet count >50 within Time, FireAlarm) (col. 6, lines 15-20). Shanklin does not specifically disclose providing a histogram to maintain the states of the sequence of packets, and update the histogram as the packets are detected. In analogous art, Etheridge discloses another system for detecting network attacks which uses a histogram to monitor which packet types are incoming, and updates the histogram when the packet arrives (p. 7, ¶ 83-84). It would have been obvious to one of ordinary skill in the art to combine the teaching of Etheridge with Shanklin, since it would provide an efficient method for the system of Shanklin to monitor the reception of packets and fire alarms when needed.

21. Referring to claim 4, Shanklin in view of Etheridge discloses the invention substantively as described in claim 3. Ethreridge further discloses a second field which a code representing states in which packets in the predefined sequence are detected (i.e. the histogram corresponding to TCP is incremented) (p. 7, ¶ 84). Shanklin-Etheridge do not specifically disclose that the histogram tracks the source addresses of the network devices, however Shanklin does disclose that the rule of counting SYN packets is *for any one host* (col. 6, lines 15-20). By this rationale, one of ordinary skill in the art would rationally assume that the source address must be somewhat correlated to the current count of SYN packets, in order to allow the scanner 11 the ability to

determine whether or not the SYN packet is part of the affected rule for a particular sender or another sender who is a verified user who should not be penalized.

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph E. Avellino whose telephone number is (571) 272-3905. The examiner can normally be reached on Monday-Friday 7:00-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joseph E. Avellino, Examiner
February 20, 2007